Cloudifornication

Indiscriminate Information Intercourse Involving Internet Infrastructure

Hoff (@Beaker) - FIRST 2010
Cloud Security Doesn't Matter

Today's Blog Reading:
Cloud Security Doesn't Matter
(Or, In The Cloud, Nobody Can Hear You Scream)

When Is NetWareCloud Shipping?
The Internet is a remarkably frail operating platform, loosely hinged on luck, politeness, ad hoc peering & transit, handshake relationships and the IP Protocol*

*It’s up more than it’s down because even the bad guys need it up to operate...
At the end of the day, we’re adding layers of abstraction/indirection to 40 year old technologies and practices & wondering why we still have issues.
There Ain't Nuthin' Wrong With The InterTubes!
The Internet assumes a fictional trusted core but is in fact an untrusted, unreliable & hostile platform.

So then, is Cloud.
Anyone Know What This Is?
More Familiar?

Pedal Assembly

Current Pedal
- Rare occurrences of excessive friction on contact points

Reinforced Pedal
- Reinforcement bar reduces surface tension and excess friction

- Precision Cut Steel Reinforcement Bar Inserted
Rare? Yes.

Rare occurrences of excessive friction on contact points.
Tragic? Absolutely.
Guess What? No Definitions Of Cloud
Provider’s/Technician’s View

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

Abstraction of Infrastructure
Resource Democratization
Services Oriented
Self-Service, On-Demand
Elasticity/Dynamism
Utility Model Of Consumption & Allocation
From the Consumer’s Perspective...

Everything Is Cloud...
CloudWow! You’ll Say “HOW?” Every Time...
The Journey to the InterCloud

Begins With a Single Slide, It Does...
...It Ends With One, Too...

...and Here It Comes...
Journey To The Intercloud Made Simple

- Virtualize Data Centers
- Stand-Alone Data Centers
- Private Cloud
- Public Cloud
- Intercloud
- Hybrid Clouds
- Virtual Private Cloud
- Cloud Brokers

Federation / Workload Portability / Interoperability
Three delivery models that people talk about when they say “Cloud”:

- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**
- **Infrastructure as a Service (IaaS)**

What Do These Look Like?
Cloud Model :: Infrastructure as a Service (IaaS)

- APIs
- Core Connectivity & Delivery
- Abstraction
- Hardware
- Facilities
Cloud Model :: Platform as a Service (PaaS)

- Integration & Middleware
- APIs
- Core Connectivity & Delivery
- Abstraction
- Hardware
- Facilities
Cloud Model :: Software as a Service (SaaS)
Packaging these up in combination yields lots of *aaS(es):

- Storage as a Service
- Database as a Service
- Information as a Service
- Process as a Service
- Integration as a Service
- Security as a Service
- Management as a Service
- Testing as a Service...

*David Linthicum: Defining the Cloud Computing Framework* http://cloudcomputing.sys-con.com/node/811519
The Many Dimensions Of Cloud :: SaaS
The Many Dimensions Of Cloud :: IaaS

- Infrastructure as a Service (IaaS)
- Security
- Features
- Extensibility
- APIs
- Core Connectivity & Delivery
- Abstraction
- Hardware
- Facilities

SaaS

PaaS

IaaS
The Cloud, It's Impact On Security and Vice-Versa
IaaS Security :: Guest/Host-Based

- Provider secures “their” infrastructure to maximize availability & multi-tenancy
- Remainder of the stack (and confidentiality, integrity) is your problem
- General focus is on VM’s & Guest-Based

IaaS Security Diagram:

- Data
- OS & Applications
- VMs/Containers

APIs
- Core Connectivity & Delivery
- Abstraction
- Hardware
- Facilities
7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet...you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content and Applications...We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.
Provider owns the compute, network, storage layers & programmatic interface security

The consumer creates the applications based upon supported development environment

Writing secure applications and ensuring your data is safe is on you
Oh, Passwords?

2.1. You must provide accurate and complete registration information any time you register to use the Service. **You are responsible for the security of your passwords and for any use of your account.** If you become aware of any unauthorized use of your password or of your account, you agree to notify Google immediately.
The provider owns the entire stack.

Security (C, I and A) becomes a contract negotiation.

Traditional security and compliance functions are more administrative & policy-focused.
8.3. Protection of Your Data. Without limiting the above, We shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data. We shall not (a) modify Your Data, (b) disclose Your Data except as compelled by law in accordance with Section 7.5 (Compelled Disclosure) or as expressly permitted in writing by You, or (c) access Your Data except to provide the Services or prevent or address service or technical problems, or at your request in connection with customer support matters.
What This Means To Security

IaaS
- Hardware
- APIs
- Facilities
- VMs/Containers
- OS & Applications

PaaS
- Integration & Middleware
- Core Connectivity & Delivery
- Abstraction
- APIs
- Hardware
- Facilities
- OS & Applications

SaaS
- Applications
- Data
- Metadata
- Content
- Presentation
- Modality

Build It In

RFP/Contract It In
So What Does That Really Mean?

- Depending upon the Cloud delivery model, many options for compensating controls are abstracted to “good enough” or are simply unavailable.

- The provider abstracts away the compute, storage and network which “simplifies” things but eliminates entire classes of capability, limiting visibility and options.

- Even with the potential for API’s and open interface standards, when it comes to Cloud we’re at the mercy of what is provided and...
It All Comes Down To Trust...

What are we going to differently about who we trust, how and why?
Heart Of Darkness ::
Corrosive (t)Rust
:: Heart Of Darkness
Corrosive (t)Rust

Virtualization & Cloud’s Operational Integrity, confidentiality and availability are based on faith and:

- Trust in providers
- Trust in protocols
- Trust in hardware
- Trust in software
- Trust in operations & people
Cloud is all about gracefully losing control.

Control is often an emotional issue we are often unprepared to deal with.

Transparency & visibility can easily make up for things that are out of your direct control.
Cloudifornication: Stacked Turtles (Er, Frogs)

- “Stacking Clouds on Clouds” and building levels of abstraction adds complexity and staggering interdependencies.
- We’re building on a very shaky foundation/weak base of frogs; one goes, they all go.
Same As It Ever Was

- Hypervisor vulnerabilities
- Lack of TCB implementations
- Lack of Standards
- Introduction of monocultures
- Information Leakage
- Substantial Downtime
- Security By Obscurity
Familiar Security Challenges

- Availability & SLA’s
- Confidentiality & Privacy
- Visibility & Manageability
- Portability & Interoperability
- Reliability & Resiliency
- Vendor Lock-in
- eDiscovery & Forensics
- Information Lifecycle
- Change Control
- Compliance
and What's Old is New(s) Again

- Access Control
- Data Leakage
- Authentication
- Encryption
- Denial Of Service/DDoS
- Key Management
- Vulnerability Management

- Application Security
- Database Security
- Storage Security
- SDLC
- Protocol Security
- Identity Management
- Risk Management
Air Deccan: Simplifying the Cloud

There is an ancient Hindi proverb that says:

“...just because you can, doesn’t mean you should...

...use duct tape to secure the wing of a Airbus 320 that flies at 36,000 feet...”

Rules Of the Road

The only thing keeping you alive are some painted yellow lines, a general agreement that everyone wants to arrive at their final destination & the trust that each will keep to their side of the road...
Rules Of the Road

The only thing keeping you alive are some painted yellow lines, a general agreement that everyone wants to arrive at their final destination & the trust that each will keep to their side of the road...
We Are Product Rich, But Solution Poor

- What’s true with VirtSec is true with Cloud, only more so. Viva Le 4 Horsemen!

- Depending upon the type of Cloud, you may not get feature parity for security.

- Your visibility and ability to deploy or have a compensating control deployed may not be possible or reasonable.

- As it stands now, the abstraction of Infrastructure is really driving the cyclic shift from physical network controls to logical/virtual & back into the host/guest
Centralized vs. Distributed

Mostly Centralized
Reliable/Fast
Mostly Distributed
Unreliable/Slow

Compute
Data
Bandwidth

Display

Web3.0/Infrastructure 2.0?/Security 1.3a?

Achtung! Divergent Models

The Cloud

Mainframes

Web2.0

Web1.0

Client/Server

The table shows the developers and security measures for different years:

<table>
<thead>
<tr>
<th>Year</th>
<th>Developers</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>CGI, PERL</td>
<td>Network firewalls, SSL</td>
</tr>
<tr>
<td>1997</td>
<td>ASP, JSP</td>
<td>Network firewalls, SSL</td>
</tr>
<tr>
<td>1998</td>
<td>EJB, J2EE, DCOM</td>
<td>Network firewalls, SSL</td>
</tr>
<tr>
<td>1999</td>
<td>SOAP, XML</td>
<td>Network firewalls, SSL</td>
</tr>
<tr>
<td>2001</td>
<td>Rest, SOA</td>
<td>Network firewalls, SSL</td>
</tr>
<tr>
<td>2003</td>
<td>Web 2.0</td>
<td>Network firewalls, SSL</td>
</tr>
</tbody>
</table>

* Credit: Gunnar Peterson
The Hamster Sine Wave of Pain...

* With Apologies to Andy Jaquith & His Hamster...
The Hamster Sine Wave of Pain...*

* With Apologies to Andy Jaquith & His Hamster...

The Security Hamster Sine Wave of Pain

* Time

Cloud

Deployment Is Here

Network Centricity
User Centricity
Information Centricity
Application Centricity
Host Centricity

Control Deployment/Investment Focus

We Are Here

* With Apologies to Andy Jaquith & His Hamster...
As we converge compute, network and storage our speeds and feed issues don’t subside, they intensify.

Integrating virtualized security capabilities at network scale becomes even more challenging: 10GbE/40GbE/100GbE... virtualized DC’s are pushing to terabit fabrics.

As we’ll see, this is a squeezing the balloon problem.
::Cloudanatomy

- **Content & Context** - Apps, Data, Metadata, Services
  - **Glue & Guts** - IPAM, IAM, BGP, DNS, SSL, PKI
  - **Sprockets & Moving Parts** - Compute, Network, Storage
Cloudanatomy

- Infrastructure
  - Metastructure
  - Infostructure
    - Content & Context - Apps, Data, Metadata, Services
    - Glue & Guts - IPAM, IAM, BGP, DNS, SSL, PKI
    - Sprockets & Moving Parts - Compute, Network, Storage
Owning the Stack

- Infostructure
- Metastructure
- Infrastructure
Cloud Happiness :: Warm & Fuzzies

The Cloud can provide the following security benefits:

- Centralized Data (sort of...)
- Segmented data/applications
- Better Logging/Accountability
- Standardized images for asset deployment
- Better Resilience to attack & streamlined incident response
- More streamlined Audit and Compliance
- Better visibility to process
- Faster deployment of applications, services, etc.
Information Intercourse?

- Clouds on Clouds on Clouds...
- Amorphous perimeters and the migration to multi-tenancy
- Socialist security & co-mingled data in multi-tenant elastic environments
- Really crusty protocols and even more stale approaches to integration
- Security becomes a question of SCALE...
Caveats

- The following is constructed to make you think
- We’re going to discuss a lot of interesting things
- Some are academic, some are practical
- Some things are specific to cloud, others not
- The names have not been changed to protect anyone, nor so they seek to impugn anyone
- Think about the big picture, not the little illustrations
An Example Is In Order...

- Imagine a fictional Public IaaS Cloud Provider...
- Let’s call them “Da Nile Web Services*”
- Virtualization, multi-tenancy & Isolation based on a VMM: Elastic Compute, Network & Storage Services...
- Let’s take a journey & imagine how what we’re going to discuss might affect this fictional provider of service

*It ain’t just a river in Egypt (or South America...)}
Physical FAIL

- Rackspace, Amazon, Google, Microsoft. Power Failures have all caused numerous data center outages
- CI Hosts - Robbery. Four Times
- Core IP Networks - FBI Seizure

*HT to Jesse Robbins: Failure Happens, CloudCamp Interop*
As large Cloud providers consolidate to mega datacenters, bandwidth, peering & transit traffic patterns will shift based on the physical location.

Mobility of NextGen Infrastructure & virtualization/Cloud tech. will exacerbate this.

Shared infrastructure increases the failure impact radius.
Infrastructure :: Shared Wavelengths

Submarine cables affected by the earthquake
Submarine cables not affected by the earthquake

Earthquake epicenter
December 26, 2006

Damaged Submarine Cable Systems
- SeaMeWe-4
- FLAG Europe-Asia

© 2007 TeleGeography Research
www.telegeography.com
The beauty of Cloud is that with infinite scale comes infinite FAIL!
:: Bit Buckets, Carrier Ethernet, MPLS and L2/3 VPNs

- Core Infrastructure Exploits
- ERNW’s Carrier Ethernet & MPLS subversion (Owning Carrier Networks)
- Carriers & the NSA’s “free email/voice archiving”
- Big, Flat L2 networks bring Old Skool l337 back. Remember Yersinia?
Some examples of Joanna Rutkowska & ITL’s work on CPU/Chipset and Virtualization subversion:

- Xen VMM Dom0 Escalation
- Xen VM escapes
- Bluepilling Xen w/nested virtualization
- Bypassing Intel’s TXT
- SMM attacks
- BIOS rootkits
Infrastructure :: VMM Monoculture
Do you have ANY idea where these images came from, who built them, and what is contained within them?
9. CONCLUSIONS

In this paper, we argue that fundamental risks arise from sharing physical infrastructure between mutually distrustful users, even when their actions are isolated through machine virtualization as within a third-party cloud compute service.

* Ristenpart, Tromer, Shacham, Savage
During World War II, German Panther tanks production was accurately estimated by Allied intelligence using statistical methods.

Guy Rosen’s concept of using AWS EC2 Resource IDs to externally count # of resources provisioned during a specific timeframe

John Oberheide’s* vMotion subversion (with extensions re: long distance VMotion over said Carrier Ethernet/MPLS)

*Oberheide, Cooke, Jahanian
Cloudburst VM Escapes* - Abusing emulated device drivers to provide host to guest escape in hosted (type 2) virtualized environments

*Kostya Kortchinsky Immunity, Inc.
• Kaminsky’s DNS attacks
• ERNW’s | Kapela & Pilosov’s BGP attacks, YouTube (Prefix Hijacking, MITM)
• Moxie Marlinspike’s SSL/TLS - Chained Certs, Null Certificate Prefix Bug, MITM, General Browser sux0r
• Sotirov et. al. Rogue CA & MD5 (...and so on, and so on...)
Each cloud is a system unto itself. There is no way to express the idea of exchanging information between distinct computing clouds because there is no way to express the idea of "another cloud." ...there is no way to express how that protection is provided and how information about it should be propagated to another cloud when the data is transferred.
There are literally dozens of competing cloud interface and API specifications & standards.

If complexity is the enemy of security, what is abstracted simplicity?
Developers want to point-click-deploy to Cloud from an IDE.
To them, Cloud is a platform with API’s & Interfaces, not infrastructure.
DevOps - Zen through Automation, Cultural Phenomenon, Operational collaboration or Abstraction as a Distraction?
Bitbucket runs on Amazon’s AWS (EC2/EBS)

Their site was down for almost 20 hours.
We were attacked. Bigtime. We had a massive flood of UDP packets coming in to our IP, basically eating away all bandwidth to the box. This explains why we couldn’t read with any sort of acceptable speed from our EBS, as that is done over the network. So, basically a massive-scale DDOS. That’s nice.

This is 16-17 hours after we reported the problem, which frankly, is a bit disheartening. Why did it take so long to discover? Oh well.
"If you single-source your infrastructure provider, one day you’re going to get your butt handed to you on a platter. The appearance of ‘infinite scale’ does not mean you’ll automagically realize ‘infinite resilience or availability’"

- Me
Misunderestimation

Infostructure

Cloud: WebAppSec v AppSec?
Information Exfiltration
CloudFlux & FastFlux
CloudBots
DDoS & EDoS - Economic Denial of Sustainability
This Sting(k)s...

OWASP Top 10

- Injection Flaws
- Cross Site Scripting
- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forgery (CSRF)
- Information Leakage & Error Handling
- Broken Authentication & Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to restrict URL access
SQUIRREL!

HACKERS
Systemic process changes that affect how users interact with services that can change at a moment’s notice.

The ‘Oops’ factor (esp. in SaaS) is going to be an issue...
Infocalypse*

**MisInfostructure**

*"Web2.x" application architecture, disguised/confused as "Cloud" but running on traditional non-elastic infrastructure that is poorly configured*

Barrett Lyon
Then There's the Other Extreme...

- All this abstraction...
- Sits atop more abstraction...
- In the form of AWS...

Heroku...
Incident Response

- How do you instantiate and operationalize an Incident Response Plan across your “infrastructure” when the bulk of it you don’t own or control?

- If we have little or no visibility into the underlying infrastructure (or in some cases even the applications) and providers don’t provide that capability, what do you do?
Forensics And/Or eDiscovery At Scale

Imagine 50,000+ Nodes, All Virtualized With:

- Highly variable workloads
- Huge volume levels
- Massive Multi-tenancy
- High Abstraction
- Encryption
- Restricted Access (customer v provider)
With technology like TPM/TXT, knowing where something is executing and by whom, is antithetical to the marketing to consumers of Public Cloud where elasticity/scale rule & location is uninteresting even given resource fluidity & multi-tenancy...
Cloud Providers

You Can't Have It Both Ways

You Can't Claim:
• Service Superiority & Availability
• Better Security
• Better Performance & Cost

Back That Up With:
• 1990’s SLA’s
• Outages & Breaches
• Lack Of Transparency

And Then Say:
• IT Goes Down, So We Can Too
• Your Expectations are Too High
• We’re Still Better...

Perception IS Reality
It Ain’t About Being New...

- People are so wrapped up in new flashy ‘sploits
- This is about being pragmatic and fixing the stuff that’s fundamentally broken & has been for some time
- Where’s the threat modeling, risk assessment and management?
Cloudification Redux

**Infostructure**
- Application/WebApp Insecurity, SQL Injection, Information Exfiltration

**Metastructure**
- BGP, SSL & DNS Hijacking

**Infrastructure**
- MPLS, Routing & Switching, Chipset & Virtualization Compromise

In Cloud, MUCH of this is out of your control...
New Solutions To Old Problems

The Realities of Today’s CloudSec Solutions Landscape:

- Whatever the provider exposes in the SaaS/PaaS/IaaS Stack
- Virtualization-Assist API’s (If Virtualized)
- Virtual Security Appliances (VM-based)
- Software in the Guest (If Virtualized)
- Integrating Appliances & Unified Computing Platforms (Network-based solutions)
- Leveraging Trusted Computing Elements
What Are We Doing About It?

- Emerging Infrastructure
- Converged Compute, Network & Storage solutions emerging
- Virtualization Platforms evolving
- IP NGN’s deploying
- Crippling Metastructure
- Struggling with Infostructure
What Are We Doing About It?

- Emerging Infrastructure
- Crippling Metastructure
- DNSSec
- BGP Extensions
- IPv6
- LISP, HIP, etc...
- Open API’s & Interfaces
- Struggling with Infostructure
What Are We Doing About It?

- Emerging Infrastructure
- Crippling Metastructure
- Struggling with Infostructure
- We still have buffer overflows
- The Browser Battle is lost
- Applying L1-6 “solutions” to Layer 7 & 8 “problems”
- Totally disconnected from Metastructure & Infrastructure
Someone Moved My Cybercheese...

- People who would not ordinarily think about security are doing so
- While we’re scrambling to adapt, we’re turning over rocks and shining lights in dark crevices
- Sure, Bad Things™ will happen
- But, Really Smart People™ are engaging in meaningful dialog & starting to work on solutions
- You’ll find that much of what you have works...perhaps just differently; setting expectations is critical
Wrapping Up...

- Attacks on and using large-scale Public Cloud providers are coming & Cloud services are already being used for $evil

- Hybrid security solutions (and more of them) are needed

- Service Transparency, Assurance & Auditability is key (CloudAudit)

- Providers have the chance to make security better. Be transparent.
We made the mess, now it’s time we started thinking about how to clean it up...
Here's How:

cloud security alliance™

http://www.CloudSecurityAlliance.org
CloudAudit

A6 - The Automated Audit, Assertion, Assessment, and Assurance API

CloudAudit and the Automated Audit, Assertion, Assessment, and Assurance API (A6)

The goal of CloudAudit (codename: A6) is to provide a common interface that allows cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance (A6) of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments and allow authorized consumers of their services to do likewise via an open, extensible and secure interface and methodology.

CloudAudit is a volunteer cross-industry effort from the best minds and talent in Cloud, networking, security, audit, assurance and architecture backgrounds.

The CloudAudit/A6 Working group was officially launched in January 2010 and has the participation of many of the largest cloud computing providers, integrators and consultants. You can find out more about CloudAudit by visiting the Forums.

Note: CloudAudit/A6 Working Group calls are being scheduled weekly starting 2/25/10 at 10am PST/1 PM EST. Please see the Forums for dial-in information and recordings from previous calls.
IF It All Comes Down To Trust...

What are we going to differently about who we trust, how and why?
Thanks

Name: Christofer HOFF

Twitter: @Beaker

Email: choff@packetfilter.com
-or-
hoffc@cisco.com [work]

Blog: www.rationalsurvivability.com

Phone: +1.978.631.0302